INTRODUCTION – This white paper is in response to the Request for Input (RFI) posted by the National Science Foundation (NSF) on 21 July 2008 to inform the five-year strategic plan for the Federal Networking and Information Technology Research & Development (NITRD) program.

The NITRD research agenda, as evidenced by the existing strategic plan, does span most of the foundational research areas in the NITRD domain. However, we feel that the relative emphasis given to those areas should be adjusted, and in particular, the cross cutting area of Cyber Physical Systems (CPS) needs to be given explicit and increased attention and budget transparency. The existing strategic plan does not identify CPS as an area, though aspects of CPS research could find a home in the existing areas, and more critically, the cross cutting challenges presented by CPS can not be adequately addressed without a holistic approach involving aspects of several of the current areas. For example, by their nature CPS tend to be, or have elements that are, safety critical, and similarly have significant security requirements. Accordingly, foundational CPS research needs to include integral high confidence, assurance, and security dimensions, rather than developing solutions and then attempting to add security, safety and assurance after the fact.

NITRD PRIORITIES – From our perspective the R&D objectives, as indicated by funding levels, are not optimally prioritized. Nearly 50% of the FY 2008 and 2009 NITRD budgets ($1.5B out of $3.3B in FY 08) are allocated to High End Computing (HEC), including Architecture, Infrastructure, and R&D. HEC is not at present an area where we feel US competitiveness is at stake. High levels of HEC funding appear to be institutional priorities of a past era. Expenditures for Human Computer Interaction and Information Management ($0.8B) also appear out of proportion relative to the need and potential gains in research and competitiveness to be attained. The Presidential Committee of Advisors on Science and Technology (PCAST) correctly pointed out the need to substantially increase the level of spending on CPS – which is not even explicitly mentioned among the programs in NITRD budget documents.

We are also concerned about the isolation of Cyber Security and Information Assurance (CSIA) from the systems domains of Human-Computer Interaction and Information Management (HCI&IM); Large Scale Networking (LSN); High Confidence Software and Systems, Social, Economic and Workforce Implications of IT (SEW); and Software Design and Productivity (SDP). CPS must include an essential CSIA program element because of the unique vulnerabilities and consequences associated with the target industries. What we need is CPS focused R&D in CSIA, tightly integrated with all other research challenges.

INDUSTRY / ACADEMIC / GOVERNMENT PARTNERSHIP – We believe that a public-private research partnership to advance the capabilities of cyber-physical systems, analogous to the European Union's ARTEMIS Embedded Computing Systems Initiative, is one way of addressing the CPS research challenge, and this could be achieved by creating Industry / University Consortia to perform pre-competitive research on industry-provided test beds. The "industrial strength" fidelity of the test beds is critical to ensuring that the research focuses on the highest payback elements of the problem space of cyber-physical systems. Consortia focused on

more applied levels have been highly successful and include USCAR (U.S. Council for Automotive Research) and AVSI (Aerospace Vehicle Systems Institute). Funding for the consortia could be assembled from: 1) Industry with Internal Research & Development investment; 2) Academia through Government funding; 3) Test bed development through Government funding.

We propose a model based upon joint work of integrated projects as opposed to loose / spontaneous collaborations. While the latter model can sometimes produce important benefits, we believe the focus needs to be the synergistic development of fundamental science directly motivated and evaluated on realistic challenge problems from industry. In this rapidly evolving field where time and resources are limited, this is the most effective way to build a core technology base. Knowledge and technology is best transitioned by people working on well defined problems using industrial strength test beds.

Industry has had a very limited voice in influencing research priorities of NITRD program. Organizations like PCAST have influence at a strategic level but they have little influence in implementation. We believe that proactive industrial participation in shaping NITRD priorities and participation in the research agenda is key to achieving breakthroughs required.

The CPS research agenda is cross cutting and spans multiple industries. Much of the research required is of a pre-competitive nature – where industry sponsored research dollars are inherently limited. The current approach of federal government sponsored research in this area has, to date, been ineffective in both addressing "industrial strength" real-world challenge problems, and creating transition pathways outside of the academic world. Greater industrial participation in executing the research agenda is critical to success and will spur the focused industrial-academic collaboration needed for significant progress. We believe that the Grand Challenge Application approach from the existing strategy has merit, but should have been made more concrete in the form of NITRD sponsored challenge problems and test beds to bring together government, industry, and academia, to provide a means of exploring the cross cutting nature of domains such as CPS and to foster cross fertilization between fundamental research and emerging problems.

An example candidate would be a CPS challenge focused on Autonomous Aerial Vehicles in the Next Generation National Airspace. This challenge problem would exercise all of the elements of CPS, including massive distribution, high assurance and certification, and security. Elements of mixed-criticality functions operating in a common compute platform and challenges associated with migration onto multi-core compute substrates are also of high interest. Such challenges would provide a fertile ground for research grounded in a critical problem whose resolution is essential to the future U.S. national security and economic prosperity.